BAB III

ANALISIS DAN DESAIN SISTEM

III.1. Analisis Permasalahan

Dalam sejarah perkembangan kriptografi, pesan rahasia dalam bentuk teks merupakan bentuk pesan rahasia paling awal. Dalam perkembangan selanjutnya, teknik enkripsi pesan rahasia dalam bentuk teks berganti dari teknik sederhana hingga enkripsi yang berbasis *digital*. Seiring perkembangan teknologi, teknik dan metode penyampaian pesan rahasia pun semakin beragam. Berbagai bentuk pesan rahasia di samping pesan teks seperti pesan *citra*, pesan *audio*, dan pesan *video* sudah umum digunakan. Seperti halnya pesan teks dalam menjaga kerahasiaannya, pesan non teks juga memerlukan teknik-teknik enkripsi yang sebisa mungkin sederhana tapi sukar dipecahkan.

Kerahasiaan pesan atau data yang dimiliki oleh seseorang merupakan hal penting dalam pengiriman pesan agar pesan tersebut hanya dapat diberikan oleh orang tertentu saja yang dapat mengakses informasi tersebut. Untuk menjaga kerahasiaan pesan diperlukan pengamanan data atau dikenal sebagai kriptografi. Kriptografi merupakan ilmu yang mempelajari cara pengamanan data dengan tujuan mencegah dari orang lain yang ingin mengetahui isinya, dengan menggunakan kode-kode dan aturan-aturan tertentu dan metode lainnya sehingga hanya orang yang berhak yang dapat mengetahui isi pesan sebenarnya. Algoritma *RSA* termasuk dalam kriptografi modern yang menggunakan plainteks, cipherteks dan kunci untuk melakukan proses enkripsi dan dekripsi dalam pengamanan data.

III.2. Strategi Pemecahan Masalah

Beberapa strategi pemecahan masalah dalam perancangan keamanan data berupa teks pada *file pdf* dengan menggunakan algoritma *RSA* ini adalah sebagai berikut:

1. Sistem pengamanan data berupa teks pada *file pdf* ini dapat digunakan pada semua perangkat yang telah *support* menggunakan *browser*.
2. Sistem yang dibangun ini digunakan untuk mengamankan data berupa teks pada *file pdf* dengan menggunakan *RSA* yang telah disandikan isinya dan menggunakan algoritma.
3. Sistem yang dibangun nantinya akan memiliki sebuah aplikasi khusus untuk mendekripsikan data berupa teks pada *file pdf*.

III.3. Algoritma RSA

RSA merupakan salah satu dari *Public Key Cryptosystem* yang sangat sering digunakan untuk memberikan kerahasiaan terhadap keaslian suatu data *digital*. Keamanan enkripsi dan dekripsi data model ini terletak pada kesulitan untuk memfaktorkan *modulus n* yang sangat besar[Sistem yang dibangun nantinya akan memiliki sebuah aplikasi khusus untuk mendeskripsikan data berupa teks pada *file pdf.*

Dalam kriptografi, *RSA* adalah algoritma untuk enkripsi kunci publik. Algoritma ini adalah algoritma pertama yang diketahui paling cocok untuk menandai (*signing*) dan untuk enkripsi dan salah satu penemuan besar pertama dalam kriptografi kunci publik. *RSA* masih digunakan secara luas dalam protokol-

protokol perdagangan *elektronik* dan dipercayai sangat aman karena diberikan kunci-kunci yang cukup panjang dan penerapan-penerapannya yang sangat mutakhir.

Algoritma pembentukan kunci :

1. Tentukan p dan q bernilai dua bilangan prima besar, acak dan dirahasiakan, p ≠ q, p dan q memiliki ukuran yang sama.
2. Hitung n = p x q, dan hitung $\phi(n) = (p - 1) \times (q - 1)$, bilangan *integer n* disebut (*RSA*) *modulus*.
3. Tentukan *e* bilangan prima acak yang memiliki syarat : $1 < e < 1(n)$, GCD(*e*, i(*n*)) = 1, disebut *e* relatif prima terhadap i(*n*), bilangan *integer* n disebut (RSA) *enciphering component*, sehingga menghasilkan $D_d (E_e(m)) = E_e(D_d(c)) \equiv m^d \bmod n$.

III.4. Implementasi Algoritma *RSA* Dalam Keamanan *File PDF*

III.4.1. Proses Enkripsi Algoritma *RSA*

Pilih nilai P dan Q, Nilai P dan Q adalah bilangan prima acak yang panjangnya 4 bit, nilai P ≠ Q. Nilai P dan Q yang dipakai dalam pengujian kedua P = 11, Q = 13.

Tentukan nilai r, N, dan E

N = P . Q = 11 . 13

N = 143

$\phi(r) = (p - 1)(q - 1) = (11-1)(13-1)$

= 120

Nilai E merupakan bilangan relatif prima acak bersifat publik, Faktor Persekutuan Terbesar dari r dan nilainya < r. E.gdc(r) = E.gdc(120) = 59

Lakukan transformasi satu ke satu untuk m (terletak pada rentang 0 – (n-1)) hal ini dilakukan agar nilai enkripsi tidak terlampau besar.

Plainteks = Tes atau 84, 101, 115 (dirubah menjadi *ASCII* desimal)

Rentang setiap blok m = 0 – (n-1) = 0 – 142

m = 84101115 $m_1 = 84$ $m_2 = 101$ $m_3 = 115$

Proses enkripsi:

$Y = m^e \bmod N$

$Y_1 = m_1^e \bmod N \equiv 84^{59} \bmod 143 \equiv 63$

$Y_2 = m_2^e \bmod N \equiv 101^{59} \bmod 143 \equiv 17$

$Y_3 = m_3^e \bmod N \equiv 115^{59} \bmod 143 \equiv 97$

Y (ciphertext)= 63 17 97.

III.4.2. Proses Dekripsi Algoritma *RSA*

Hitung nilai D, D dengan memasukkan nilai m satu persatu sampai hasilnya bulat, nilai D bersifat rahasia.

E .D mod r = 1

$E.D \equiv 1 \bmod r$

D = 1 (x . r)/E = 1 (m. 120)/59

Dengan mencoba nilai x = 1, 2, 3, 4, ... diperoleh nilai x yang menghasilkan D yang bulat adalah 29. Dan nilai D yang didapat adalah 59.

D = 1 (x . r)/E = 1 (29. 120)/E 59

= 3840/59 = 59

Setelah nilai D didapat langkah selanjutnya ialah mengubah *ciphertext* kembali ke teks awal.

Y = 63 17 97 (Y1 = 63 Y2 = 17 Y3 = 97)

$m = Y^D \bmod N$

$m1 = Y_1^{\ D} \bmod N \equiv 63^{59} \bmod 143 \equiv 84$

$m2 = Y_2^{\ D} \bmod N \equiv 17^{59} \bmod 143 \equiv 101$

$m3 = Y_3^{\ D} \bmod N \equiv 97^{59} \bmod 143 \equiv 115$

Sehingga, nilai m = 84 101 115 apabila dikonversikan menjadi string kembali berdasarkan tabel *ASCII* maka akan menghasilkan teks asli “Tes”.

III.5. Perancangan

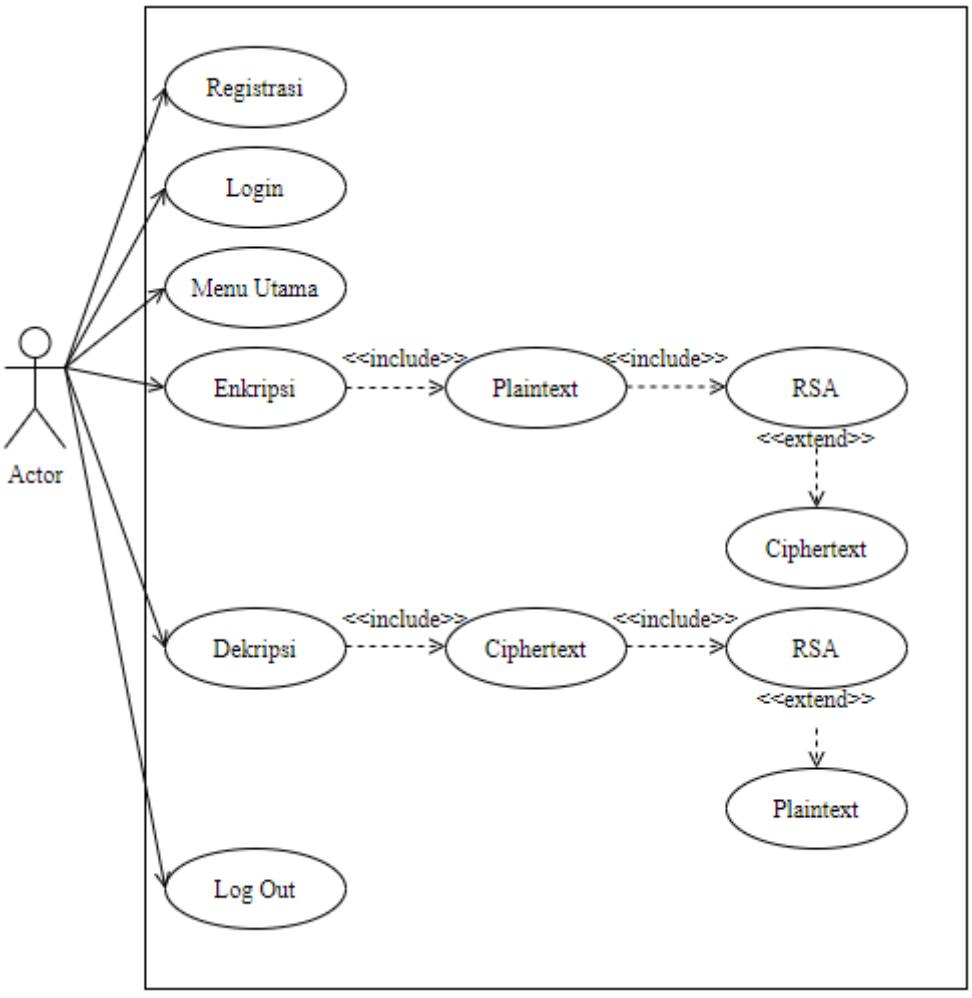
Perancangan aplikasi merupakan perancangan yang dilakukan untuk merancang sebuah aplikasi dengan menggunakan salah satu bahasa pemrograman *PHP*, dalam kasus ini penulis merancang sebuah aplikasi keamanan data *file pdf* dengan menggunakan *PHP*. Aplikasi ini bersifat *Kriftografi*, tugas utama aplikasi ini adalah enkripsi dan dekripsi *file pdf.*

III.6. Desain Sistem

Perancangan ini akan memberikan penjelasan mengenai rancangan aplikasi serta pembentukan dan pembangunan aplikasi kriptografi algoritma *RSA* dalam mengamankan data *file pdf.*

III.6.1. *Use Case Diagram*

Perilaku beserta tugas-tugas dari tiap–tiap elemen maupun aktor yang terlibat dalam sistem yang akan dirancang, akan digambarkan dalam diagram *use case* yang bertujuan untuk memberikan gambaran secara umum tentang sistem yang akan dirancang gambar III.1 sebagai berikut:



Gambar III.1. ***Use Case Diagram***

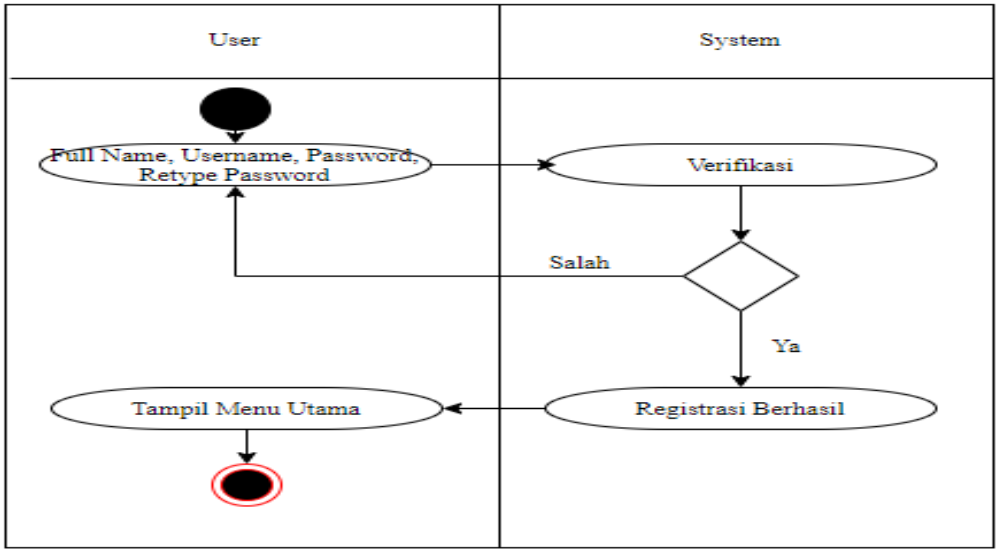
Contoh Alur: Pertama user akan registrasi terlebih dahulu, jika sudah punya akun langsung login saja, lalu masuk ke menu enkripsi user akan memasukan file yang akan menjadi plainteks, setelah terenkrip dan menghasilkan cipherteks user akan

masuk ke menu dekripsi dan memasukkan cipherteks, setelah terdekrip dan menjadi palinteks user akan log out.

III.6.2. *Activity Diagram*

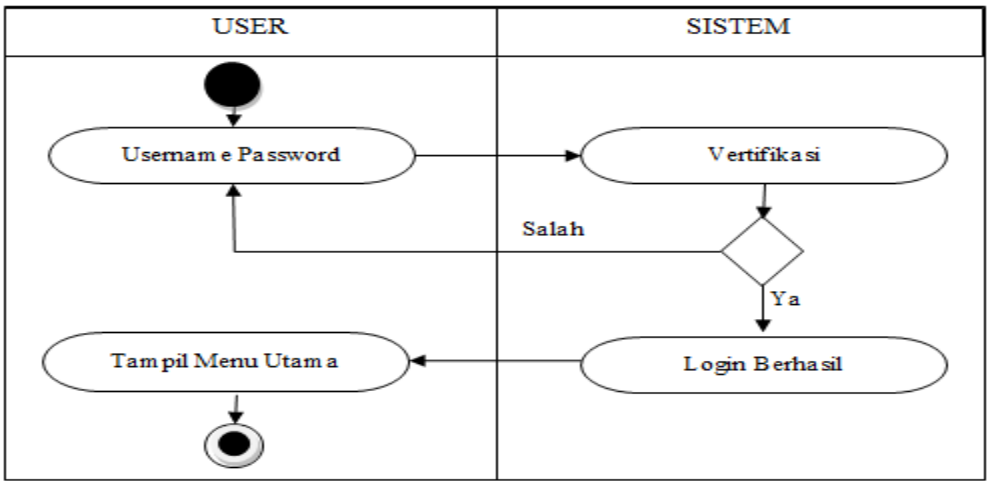
Activity Diagram menggambarkan berbagai alir aktivitas, bagaimana masing-masing alir berawal, *decision* (keputusan) yang mungkin terjadi, dan bagaimana sebuah sistem berakhir.

III.6.2.1. *Activity Diagram* Registrasi



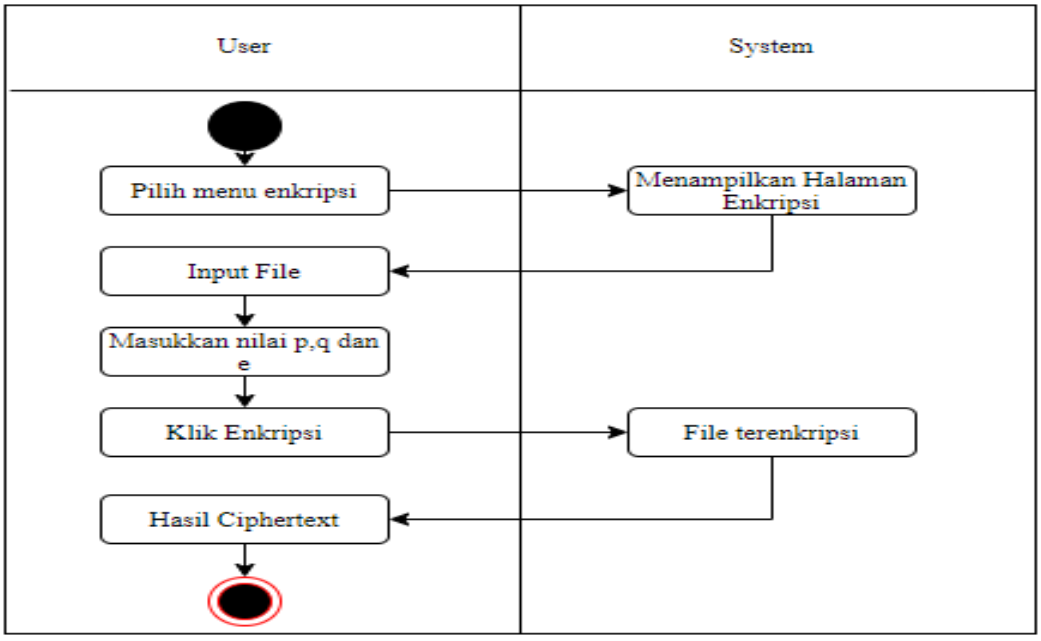
Gambar III.2. *Activity* Diagram Registrasi

III.6.2.2 *Activity Diagram Login*



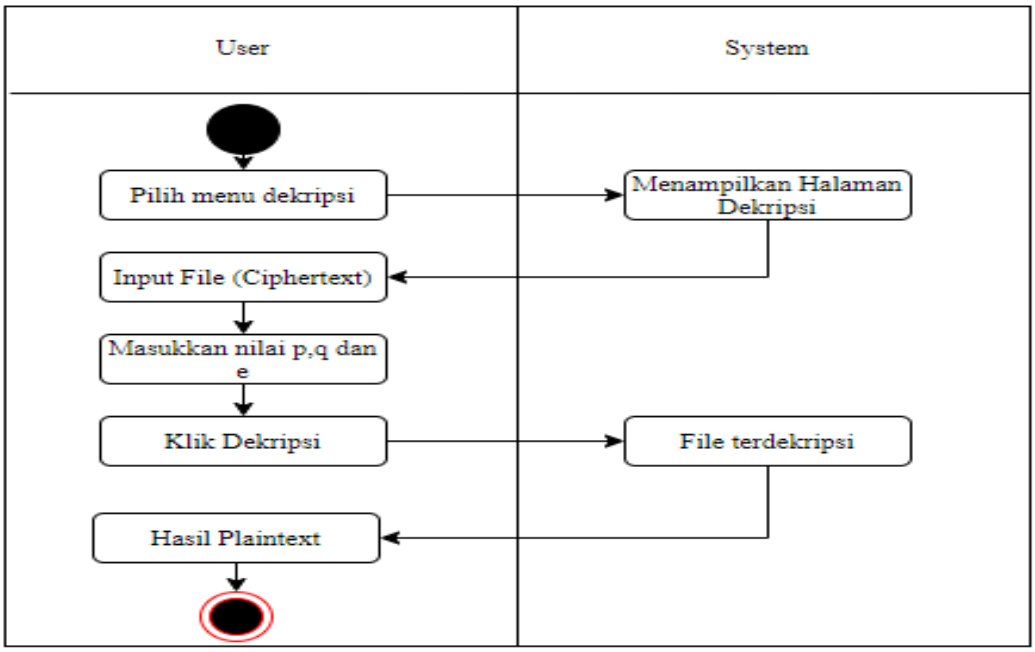
Gambar III.3. *Activity* Diagram *Login*

III.6.2.3 *Activity Diagram* Enkripsi *RSA*



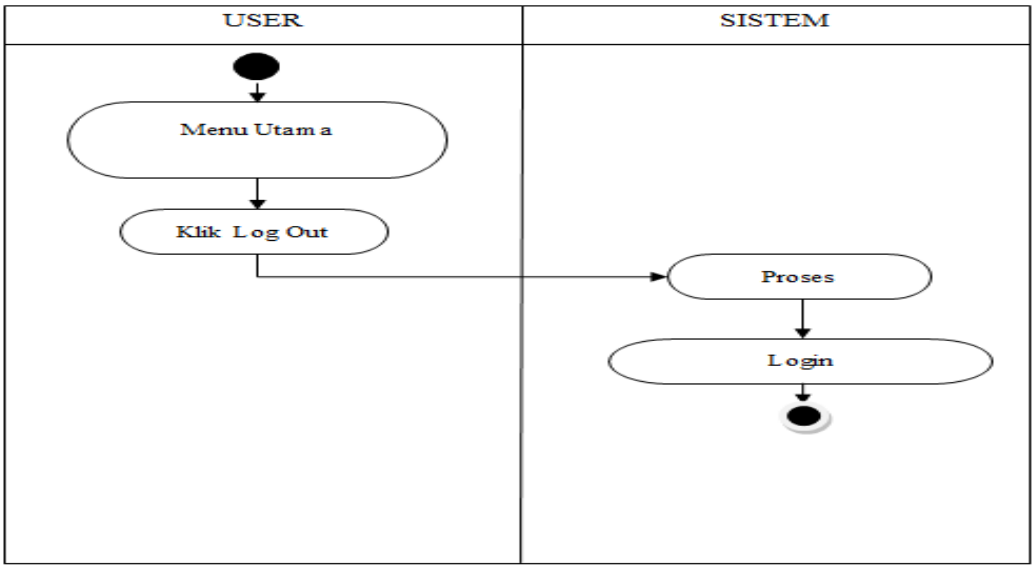
Gambar III.4. *Activity* Diagram Enkripsi *RSA*

III.6.2.4 *Activity Diagram* Dekripsi *RSA*



Gambar III.5. *Activity* Diagram Dekripsi *RSA*

III.6.2.5 *Activity Diagram* Log Out



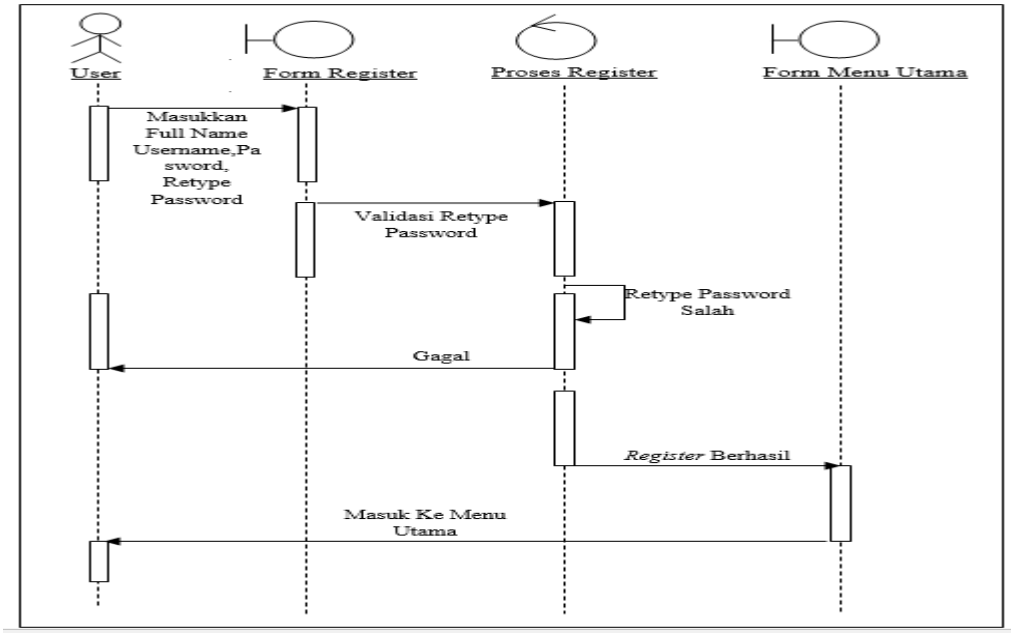
Gambar III.6. *Activity Diagram* Log Out

III.6.3. *Sequence Diagram*

Sequence Diagram adalah suatu diagram yang memperlihatkan atau menampilkan interaksi-interaksi antar objek di dalam sistem yang disusun pada sebuah urutan atau rangkaian waktu. Interaksi antar objek tersebut termasuk pengguna, *display*, dan sebagainya berupa pesan/*message*.

III.6.3.1. *Sequence Diagram* Registrasi

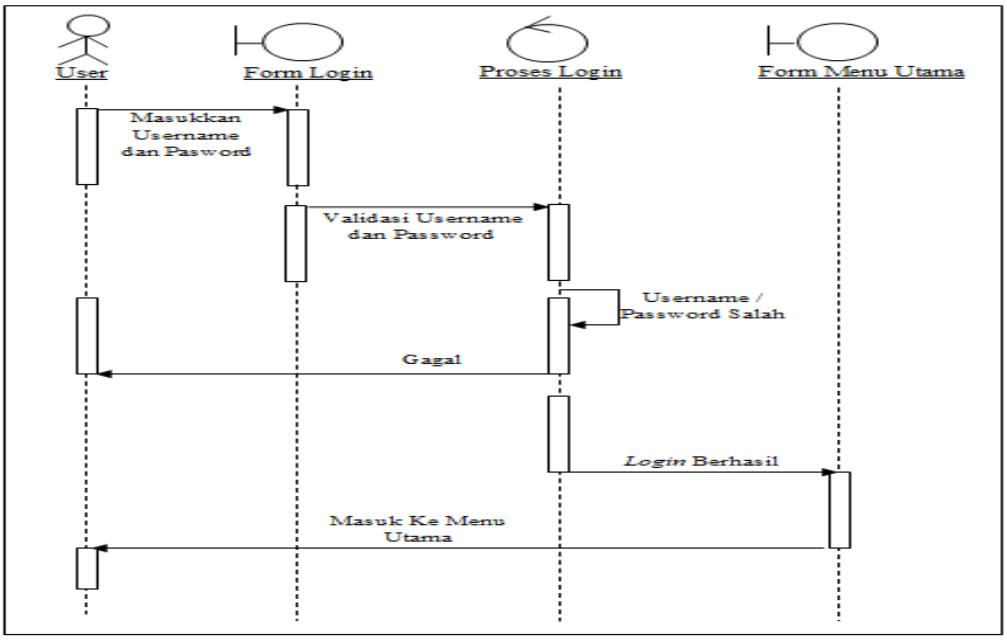
Serangkaian kerja melakukan Registrasi dapat dilihat pada Gambar III.7 dibawah ini.



Gambar III.7. *Sequence Diagram Register*

III.6.3.2. *Sequence Diagram* Login

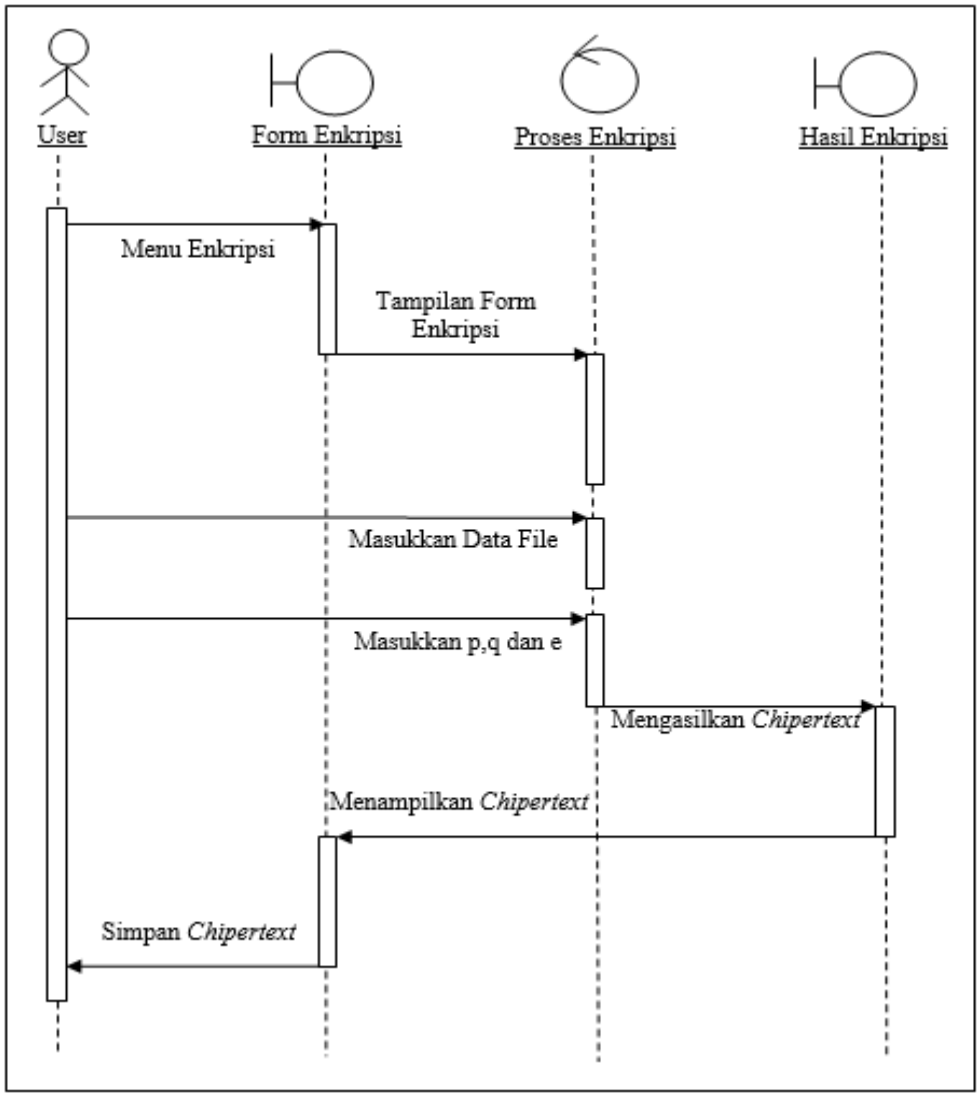
Serangkaian kerja melakukan *Login* dapat dilihat pada Gambar III.8 dibawah ini .



Gambar III.8. *Sequence Diagram Login*

III.6.3.3. *Sequence Diagram* Enkripsi *RSA*

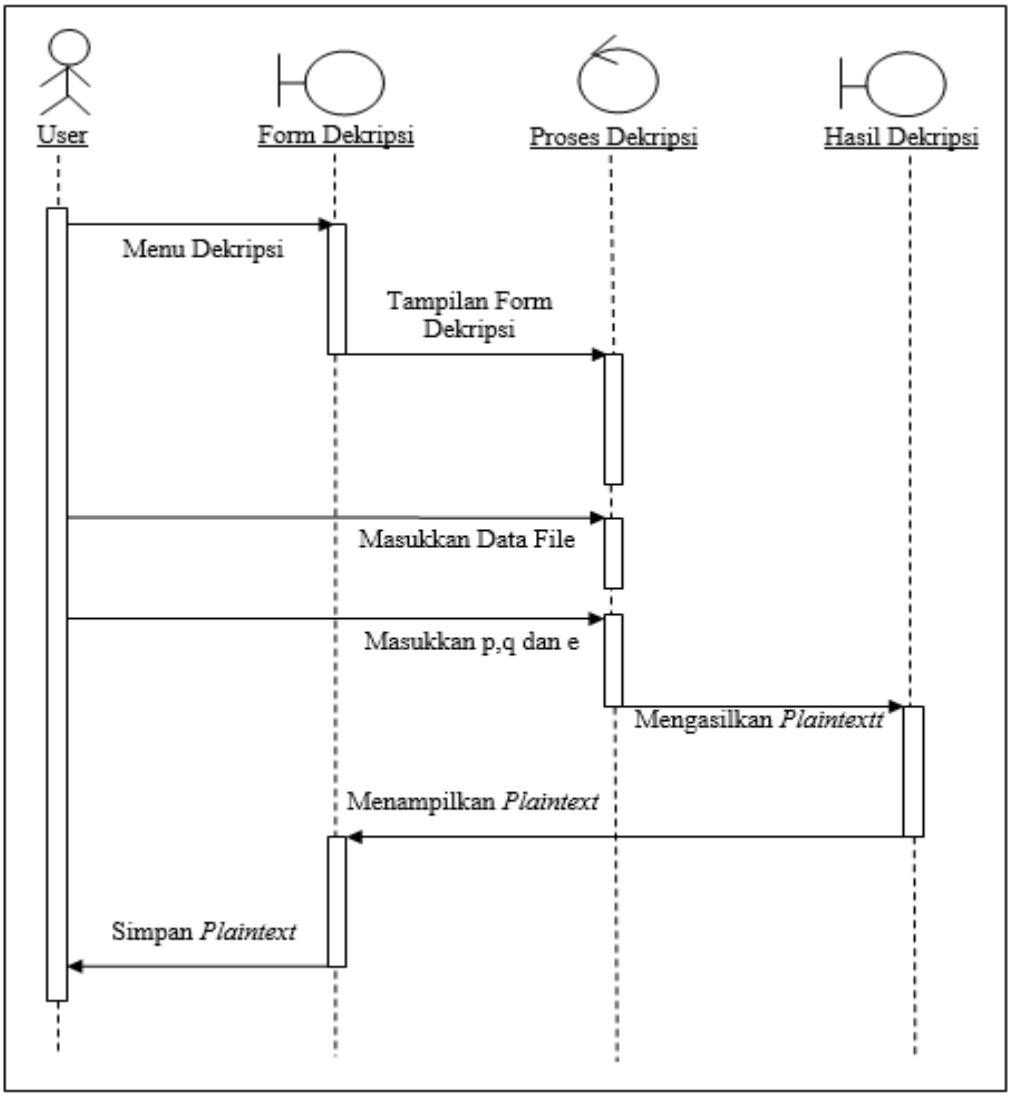
Serangkaian kerja melakukan enkripsi *RSA* dapat dilihat pada Gambar III.9. dibawah ini.



Gambar III.9. *Sequence Diagram* Enkripsi *RSA*

III.6.3.4. *Sequence Diagram* Dekripsi *RSA*

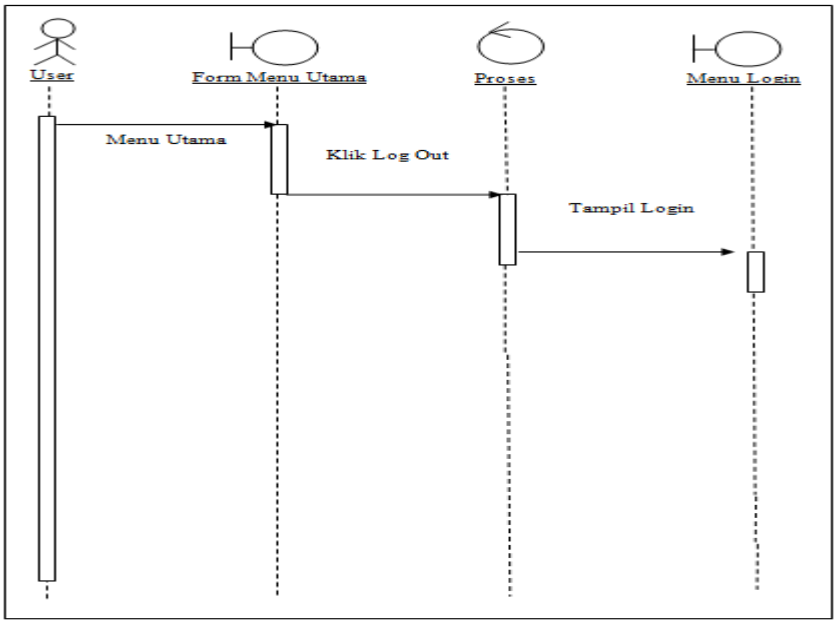
Serangkaian kerja melakukan dekripsi *RSA* dapat dilihat pada Gambar III.10 dibawah ini.



Gambar III.10. *Sequence Diagram* Dekripsi Dan *RSA*

III.6.3.5. *Sequence Diagram* Log Out

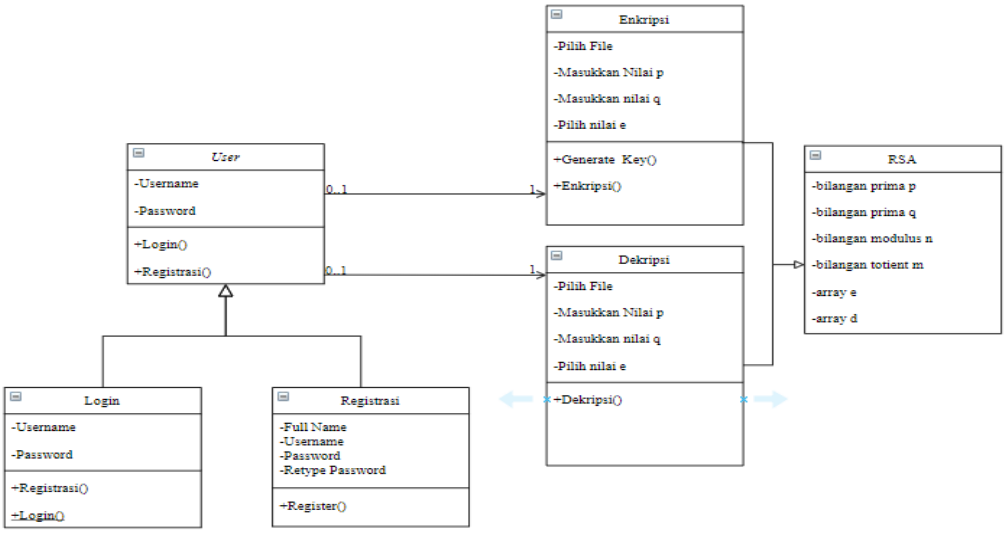
Serangkaian kerja melakukan *log out* dapat dilihat pada Gambar III.11 dibawah



Gambar III.11. *Sequence Diagram Log Out*

III.6.4 *Class* Diagram

Class Diagram Keamanan data berupa teks pada *file pdf* dengan menggunakan algoritma *RSA* dan dapat dilihat pada Gambar III.12.

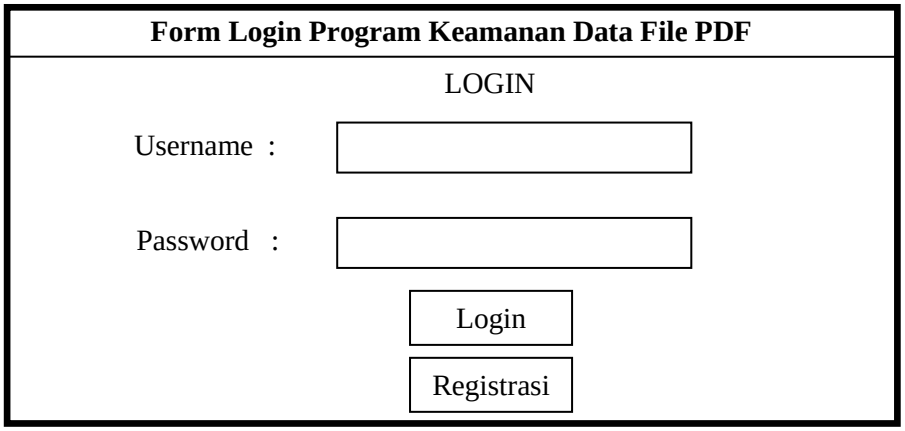


Gambar III.12. *Class Diagram* Keamanan Data *File PDF RSA*

III.7. Desain *Interface*

III.7.1. Perancangan *Form Login*

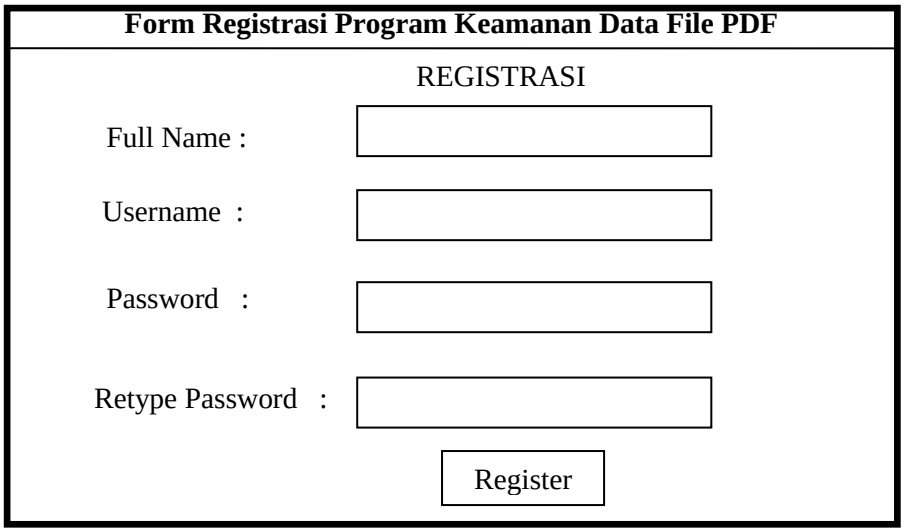
Perancangan *form login* ini terdiri dari empat buah *label*, dua buah *button* dan dua buah *textfield*. Untuk lebih jelasnya, perancangan *form login* dapat dilihat pada Gambar III.13 sebagai berikut:.



Gambar III.13. Perancangan *Form Login*

III.7.2. Perancangan *Form* Registrasi

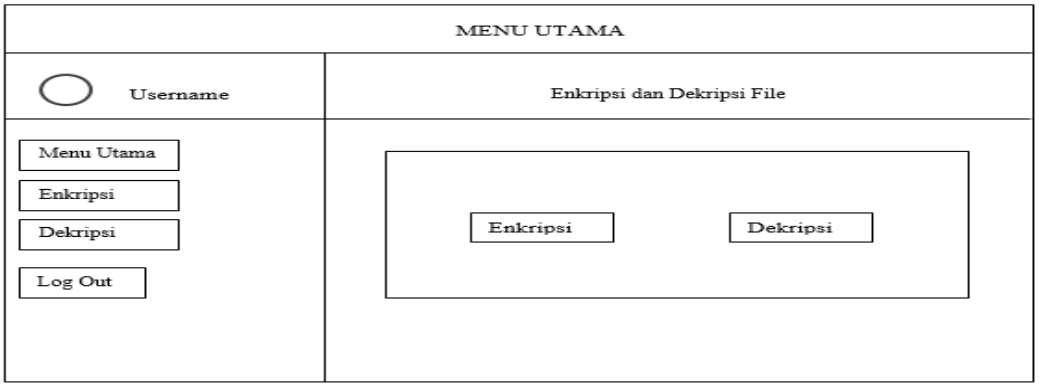
Perancangan *form Registrasi* ini terdiri dari lima buah *label*, satu buah *button* dan empat buah *textfield*. Untuk lebih jelasnya, perancangan *form registrasi* dapat dilihat pada Gambar III.14 sebagai berikut:.



Gambar III.14. Perancangan *Form Registrasi*

III.7.3. Perancangan *Menu* Utama

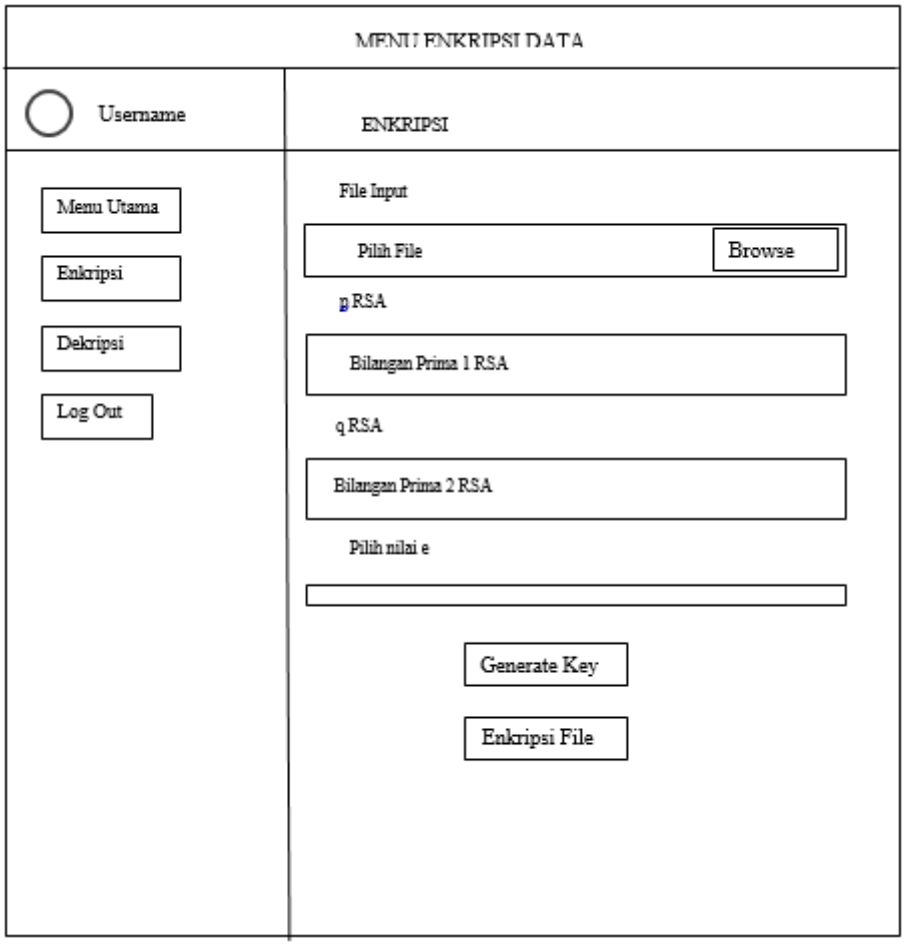
Perancangan *Menu* Utama ini terdiri dari empat buah *button*, dua buah *label*, dan satu buah *textfield*. Untuk lebih jelasnya, perancangan *Menu* Utama dapat dilihat pada Gambar III.15 sebagai berikut:



Gambar III.15. Perancangan *Menu* Utama

III.7.4. Perancangan *Menu* Enkripsi *RSA*

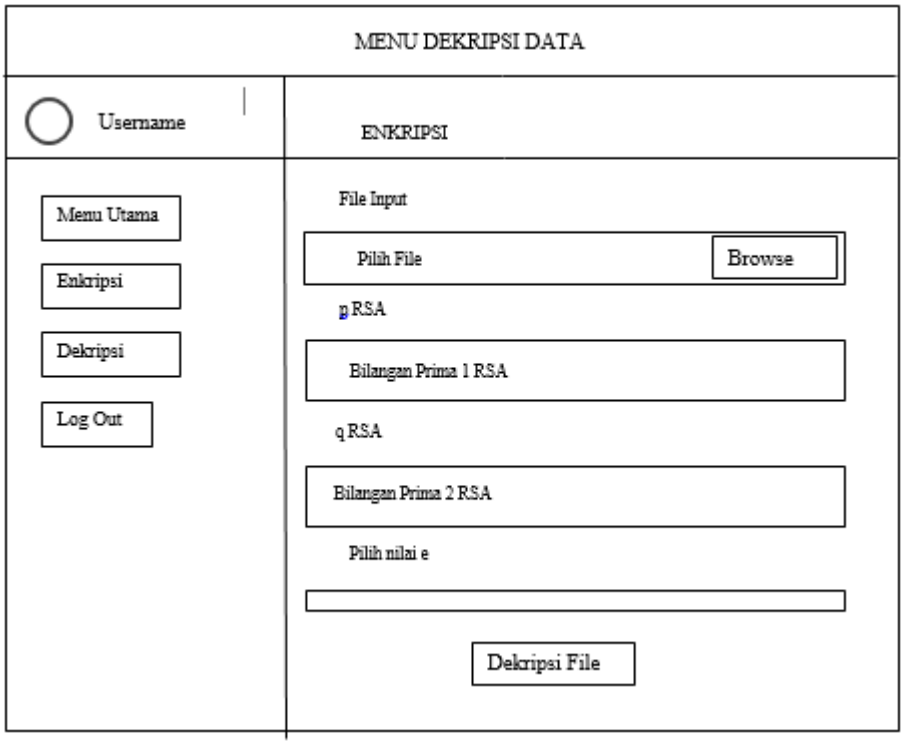
Perancangan *Menu* Enkripsi *RSA*, untuk lebih jelasnya, perancangan *Menu* Enkripsi dapat dilihat pada Gambar III.16 sebagai berikut:



Gambar III.16. Perancangan *Menu* Enkripsi *RSA*

III.7.5. Perancangan *Menu* Dekripsi *RSA*

Perancangan *Menu* Dekripsi *RSA*, untuk lebih jelasnya, perancangan *Menu* Dekripsi dapat dilihat pada Gambar III.17 sebagai berikut:



Gambar III.17. Perancangan *Menu* Dekripsi *RSA*